UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,509	12/19/2001	Richard E. Kessler	005655.P004	6406

8791 7590 02/24/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/025,509	KESSLER ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/21/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 16-18, 20-22 and 24 are rejected under 35 U.S.C. 102(e) as being anticipated by Blaker et al. United States Publication Number 2002/0004904.

As per claim 16:

Blaker et al. teach an apparatus comprising:

a first processor to call a macro security operation to establish a secure session; (Page2, paragraph 11)

a second processor coupled to the first processor, the second processor to perform a plurality of primitive security operations in response to the macro security operation call; (Page 2, paragraph 11) and a memory coupled to the first and the

second processor, the memory to store a set of data generated by the second processor. (Figure 1, 36 and 22; Page 2, paragraph 11; Page 3, paragraph 34)

As per claim 17:

Blaker et al. teach all the subject matter as disclosed above. In addition, Blaker et al. further disclose an apparatus wherein the second processor comprises: a request unit to fetch and to distribute the macro security operation; (Page 3, paragraph 34) and a plurality of execution units coupled to the request unit, one of the plurality of execution units to execute the plurality of primitive security operations. (Page 3, paragraph 34)

As per claim 18:

Blaker et al. teach all the subject matter as disclosed above. In addition, Blaker et al. further disclose an apparatus wherein comprising: the first processor to call a second macro security operation after calling the first macro security operation; (Page 3, paragraph 39) and a second one of the plurality of execution units to execute a second plurality of primitive security operations corresponding to the second macro security operation before the one of the plurality of execution units completes execution of the plurality of primitive security operations. (Page 3, paragraph 39)

As per claim 20:

Blaker et al. teach all the subject matter as disclosed above. In addition, Blaker et al. further disclose an apparatus further comprising the memory to store a set of source data. (Figure 1, 36 and 22)

As per claim 21:

Blaker et al. teach an apparatus comprising:

a first processor to call a macro security operation; (Page2, paragraph 11)

a second processor coupled to the first processor, the second processor comprising a request unit to retrieve the macro security operation, a plurality of execution units coupled to the request unit, one of the plurality of execution units to perform a plurality of primitive security operations, the plurality of primitive security operations corresponding to the macro security operation; (Page 2, paragraph 11; Page 3 pragraphs 34 and 39) and

a memory coupled to the first and second processor, the memory to store a set of data generated by the second processor. (Figure 1, 36 and 22; Page 2, paragraph 11)

As per claim 22:

Blaker et al. teach all the subject matter as disclosed above. In addition, Blaker et al. further disclose an apparatus further comprising the memory to store a set of source data from the host processor. (Figure 1, 22 and 36)

As per claim 24:

Blaker et al. teach all the subject matter as disclosed above. In addition, Blaker et al. further disclose an apparatus comprising:

the first processor to call a primitive security operation; (Page2, paragraph 11) and

a second one of the plurality of execution units to execute the primitive security operations. (Page 2, paragraph 11)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1-15 and 25-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blaker et al. United States Publication Number 2002/0004904 in view of Bellwood et al. United States Letter Patent Number 6,584,567.

As per claim 1:

Blaker et al. teach a computer implemented method comprising:

calling an operation from a first processor; (Page 2, paragraph 11; one or more operands are downloaded ...from the system memory)

executing a plurality of primitive security operations at a second processor in response to the operation call; (Page 2, paragraph 11)

generating a set of data from executing the plurality of primitive security operations; (Page 2, paragraph 11) and

Blaker et al. do not explicitly disclose establishing a secure session with the set of data.

Bellwood et al. in analogous art, however, disclose a method of establishing a secure session between client browser and a server. (Col. 2, lines 19-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker et al. to include a method of establishing a secure session with the set of data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Bellwood et al. (Col. 1, lines 56-58) in order to provide a mechanism that reduces network resource demands and enhancing secure communication between devices.

As per claim 2:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a computer implemented method wherein the set of data comprises:

a set of decrypted data; (Page 6, paragraph 54)

a set of encrypted data; (Page 6, paragraph 54) and

a set of hashed messages. (Page 6, paragraph 54)

As per claim 3:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a computer implemented method comprising a set of random numbers. (Page 4, paragraph 34)

As per claim 4:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a computer implemented method comprising the first processor calling a second operation to establish a second secure session. (Col. 2, lines 49-50)

As per claim 5:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a computer implemented method wherein the secure session is an SSL 3.0 session, a TLS session, or an IPSec session. (Col. 3, lines 50-59)

As per claim 6:

Blaker et al. teach a computer implemented method comprising:

calling a macro security operation; (Page 2, paragraph 11; one or more operands are downloaded ...from the system memory)

performing a set of operations in response to the macro security operation, (Page 2, paragraph 11)

Blaker et al. do not explicitly disclose the set of operations comprising:

generating a secret and a key material, creating a first finished hash for a client

message, creating a second finished hash for a server message, creating a finished message; and establishing a secure session.

Bellwood et al. in analogous art, however, disclose a method of

generating a secret and a key material, (Col. 9, lines 2-5)

creating a first finished hash for a client message, (Figures 3A and 3B; Col. 9, lines 6-10)

creating a second finished hash for a server message, (Figures 3A and 3B; Col. 9, lines 6-10)

creating a finished message; (Figures 3A and 3B) and

establishing a secure session. (Col. 2, lines 19-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker et al. to include a method of establishing a secure session. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Bellwood et al. (Col. 1, lines 56-58) in order to provide a mechanism that reduces network resource demands and enhancing secure communication between devices.

As per claim 7:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a computer implemented method wherein the set of operations further comprises decrypting a pre-master secret; and decrypting a client finished message. (Col. 9, lines 1-5)

As per claim 8:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a computer implemented method wherein the set of operations further comprises generating a set of random numbers. (Page 4, paragraph 34)

As per claim 9:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a computer implemented method wherein the set of operations further comprises creating an expected finished message. (Figures 3A and 3B)

As per claim 10:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a computer implemented method comprising calling a second macro security operation to establish a second secure session. (Col. 2, lines 49-50)

As per claim 11:

Bellwood et al. teach a system comprising:

a first network element to request a secure session; (Col. 5, lines 30-31, Bellwood) and

a second network element networked to the first network element, the second network element to call a macro security operation from a first processor, (Col. 5, lines 32-37, Bellwood)

Bellwood et al. do not explicitly disclose executing a plurality of primitive security operations at a second processor in response to the macro security operation call and to generate a set of data from the execution of the plurality of primitive security operations.

Blaker et al. in analogous art, however, disclose a method of executing a plurality of primitive security operations at a second processor in response to the macro security operation call and to generate a set of data from the execution of the plurality of primitive security operations. (Page 2, paragraph 11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Bellwood et al. to include a method of executing a plurality of primitive security operations at a second processor in response to the macro security operation call and to generate a set of data from the execution of the plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Blaker et al. (Page 1, paragraph 4) in order to allow a host processor to download one or more command and instruct the co-processor to execute one or more of the downloaded commands. This way, the host processor will have more time available to attend other tasks.

As per claim 12:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a system wherein the set of data comprises: a

set of decrypted data; a set of encrypted data; and a set of hashed data. (Page 6, paragraph 54)

As per claim 13:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a system wherein the first network element to request the secure session comprises the first network element to transmit a set of messages to the second network element, (Col. 5, lines 30-31, Bellwood) to execute a second macro security operation, and to generate a second set of data from the execution of the second macro security operation. (Col. 5, lines 41-53; ...the client opening a second secure session to the proxy ..., Bellwood)

As per claim 14:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a system comprising a third network element networked to the second network element, the third network element to request a second secure session with the second network element. (Col. 4, lines 65-67 and Col. 5, lines 1-2)

As per claim 15:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a system comprising: the first network element to request a second secure session with the second network element; and the second network element to execute a second macro security operation to establish the second secure session with the first network element. (Col. 2, lines 49-50)

As per claim 25:

Blaker et al. teach a machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

executing a macro security operation at a first one of the set of processors; (Page 2, paragraph 11)

executing a plurality of primitive security operations at a second one of the set of processors in response to the macro security operation call; (Page 2, paragraph 11)

generating a set of data from executing the plurality of primitive security operations; (Page 2, paragraph 11) and

Blaker et al. do not explicitly disclose establishing a secure session with the set of data.

Bellwood et al. in analogous art, however, disclose a method of establishing a secure session between client browser and a server. (Col. 2, lines 19-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker et al. to include a method of establishing a secure session with the set of data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Bellwood et al. (Col. 1, lines 56-58) in order to provide a mechanism that reduces network resource demands and enhancing secure communication between devices.

As per claim 26:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a machine-readable medium wherein the set of data comprises:

a set of decrypted data; (Page 6, paragraph 54)

a set of encrypted data; (Page 6, paragraph 54) and

a set of hashed messages. (Page 6, paragraph 54)

As per claim 27:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a machine-readable medium wherein the set of data comprises a set of random numbers. (Page 4, paragraph 34)

As per claim 28:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a machine-readable medium comprising the first processor calling a second operation to establish a second secure session. (Col. 2, lines 49-50)

As per claim 29:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a machine-readable medium wherein the secure session is an SSL 3.0 session, a TLS session, or an IPSec session. (Col. 3, lines 50-59)

As per claim 30:

Blaker et al. teach a machine-readable medium that provides instructions, which when executed by a set of one or more processors, cause said set of processors to perform operations comprising:

calling a macro security operation from a first one of the set of processors; (Page 2, paragraph 11)

performing a set of operations at a second one of the set of processors in response to the macro security operation, (Page 2, paragraph 11)

Blaker et al. do not explicitly disclose the set of operations comprising: generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, creating a finished message; and establishing a secure session.

Bellwood et al. in analogous art, however, disclose a method of

generating a secret and a key material, (Col. 9, lines 2-5)

creating a first finished hash for a client message, (Figures 3A and 3B; Col. 9, lines 6-10)

creating a second finished hash for a server message, (Figures 3A and 3B; Col. 9, lines 6-10)

creating a finished message; (Figures 3A and 3B) and

establishing a secure session between client browser and a server. (Col. 2, lines 19-22).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker et

al. to include a set of operations comprising: generating a secret and a key material, creating a first finished hash for a client message, creating a second finished hash for a server message, creating a finished message; and establishing a secure session. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Bellwood et al. (Col. 1, lines 56-58) in order to provide a mechanism that reduces network resource demands and enhancing secure communication between devices.

As per claim 31:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a machine-readable medium wherein the set of operations further comprises decrypting a pre-master secret and a client finished message. (Col. 9, lines 1-5)

As per claim 32:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose a machine-readable medium wherein the set of operations further comprises generating a set of random numbers. (Page 4, paragraph 34)

As per claim 33:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a machine-readable medium comprising creating an expected finished message. (Figure 3A and 3B)

As per claim 34:

Blaker et al. and Bellwood et al. teach all the subject matter as discussed above. In addition, Bellwood et al. further disclose a machine-readable medium comprising calling a second macro security operation to establish a second secure session. (Col. 2, lines 49-50)

6. Claims 19 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blaker et al. United States Publication Number 2002/0004904 further in view of Tremblay et al. United States Letter Patent Number 5,925,123.

As per claim 19 and 23:

Blaker et al. teach all the subject matter as discussed above. In addition, Blaker et al. further disclose an apparatus wherein:

an execution queue unit coupled to the microcode unit, the execution queue unit to queue the plurality of primitive security operations; (Figure 1, 44 and 46; Page 3, paragraph 34)

a plurality of primitive security operation units coupled to the execution queue unit, the plurality of primitive security operation units to perform the plurality of primitive security operations; (Page 3, paragraph 39) and

a bus coupled to the plurality of primitive security operation units, the bus to transmit data. (Figure 1, 24; Page 3, paragraph 33)

Blaker et al. do not explicitly disclose an apparatus comprising a microcode unit to translate the macro security operation into a plurality of primitive security operations;

Tremblay et al. in analogous art, however, disclose an apparatus wherein the one of the plurality of execution units comprises: a microcode unit to translate the macro security operation into a plurality of primitive security operations; (Col. 3, lines 21-27)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Blaker et al. to include a microcode unit to translate the macro security operation into a plurality of primitive security operations. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Tremblay et al. (Abstract) in order to provide a dual instruction set processor that is capable of executing instruction in two different instructions sets from two different sources.

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay SG
Examiner
Art Unit 2133

02/18/05

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100